

IN THE CLAIMS

Please amend the claims as follows:

Claim 1 (Currently Amended): A method for storing and enabling access to data at a server, the method comprising:

~~obtaining~~ receiving a hint at the server from a first device, the hint generated by executable code located on the first device;

~~obtaining a password;~~

receiving, at the server, data encrypted by using a key, the key generated by
performing a hashing algorithm on the hint and ~~[[the]]~~ a password ~~to generate a key;~~

~~encrypting data using the key;~~

~~sending the encrypted data to a server for storage; and~~

sending the hint to a ~~client~~ second device.

Claim 2 (Original): The method of claim 1, wherein the step of performing a hashing algorithm includes hashing the password.

Claim 3 (Currently Amended): A method for storing and enabling access to data at a server, the method comprising:

~~obtaining~~ receiving a hint at the server from a first device, the hint generated by executable code located on the first device; and

~~obtaining a password;~~

receiving, at the server, data encrypted by using a key, the key generated by
performing a hashing algorithm on the hint and ~~[[the]]~~ a password ~~to generate a key, wherein~~
~~the step of~~

performing ~~[[a]]~~ the hashing algorithm includes hashing the password to derive a first secret, hashing the first secret to derive a second secret, hashing the hint and the first secret to generate an intermediate index, and hashing the intermediate index and the second secret to generate the key;

~~encrypting data using the key; and~~

~~sending the encrypted data to a server for storage.~~

Claim 4 (Currently Amended): A system, comprising:

a user interface ~~for obtaining~~ configured to obtain a password;

a key generator coupled to the user interface ~~for performing~~ configured to perform a hashing algorithm on a hint and the password to generate a key;

an encryption engine coupled to the key generator ~~for encrypting~~ configured to encrypt data stored on a device using the key;

a communications module coupled to the encryption engine ~~for sending~~ configured to send the encrypted data and the hint to a server for storage.

Claim 5 (Currently Amended): The system of claim 4, further comprising:

a hint generator ~~for generating~~ configured to generate the hint.

Claim 6 (Original): The system of claim 4, wherein the key generator hashes the password.

Claim 7 (Currently Amended): A system, comprising:

a user interface ~~for obtaining~~ configured to obtain a password;

a key generator coupled to the user interface ~~for performing~~ configured to perform a hashing algorithm on a hint and the password to generate a key wherein the key generator hashes the password to derive a first secret, hashes the first secret to derive a second secret, hashes the hint and the first secret to generate an intermediate index, and hashes the intermediate index and the second secret to generate the key;

an encryption engine coupled to the key generator ~~for encrypting~~ configured to encrypt data stored on a device using the key; and

a communications module coupled to the engine ~~for sending~~ configured to send the encrypted data to a server for storage.

Claim 8 (Currently Amended): A system, comprising:
means for obtaining a hint;
means for obtaining a password through and interface to executable code transmitted to a device;
means for performing a hashing algorithm on the hint and the password to generate a key;
means for encrypting data stored on the device using the key; and
means for sending the encrypted data to a server for storage; and
~~means for sending the hint to a client.~~

Claim 9 (Currently Amended): The system of claim 8, wherein the ~~system includes~~ executable code is stored on a computer-readable storage medium.

Claim 10 (Currently Amended): The system of claim 8, wherein the system ~~includes~~ is configured to transmit the executable code embodied in a carrier wave.

Claim 11 (Currently Amended): A method for storing and enabling access to data at a server, the method comprising:

receiving, at the server, a request to store encrypted data from a ~~client device~~;

~~sending a request to store encrypted data from a client;~~

sending an encryption downloadable to the device for deriving a key to encrypt data ~~to the client stored at the device~~;

receiving, at the server, encrypted data ~~that was encrypted by the encryption~~ downloadable from the ~~client device~~; and

~~obtaining~~ receiving, from the device, a hint, corresponding to the encrypted data and ~~needed-used~~ for regenerating the key; and

storing the hint and the encrypted data at the server.

Claim 12 (Currently Amended): A system, comprising:

an encryption downloadable ~~for deriving~~ configured to derive an encryption key from a password and a hint;

a web server ~~for interfacing configured to interface with a client, for sending device~~ and send the encryption downloadable to the ~~client device~~, and ~~for receiving encrypted~~ receive data ~~that was encrypted by the encryption downloadable from the client device~~; and

a memory coupled to the web server for storing configured to store a hint corresponding to the encrypted data and ~~needed-used~~ to regenerate the key from the client and the encrypted data.

Claim 13 (Currently Amended): A method, comprising;
~~obtaining a password;~~
~~sending-receiving, at a device,~~ encrypted data and a hint corresponding to the
encrypted data from a server ~~to a client;~~ and
inputting a password through an interface to executable code; and
performing a hashing algorithm on the password and the hint at the ~~client~~ device to
generate a key for decrypting the encrypted data.

Claim 14 (Currently Amended): The method of claim 13, wherein ~~the step of~~
performing ~~[[a]]~~ the hashing algorithm further includes hashing the password.

Claim 15 (Currently Amended): ~~[[a]]~~ A system, comprising:
a user interface ~~for obtaining~~ configured to obtain a password;
a communication module ~~for sending~~ configured to send encrypted data and a hint
corresponding to the encrypted data from a server to a ~~client~~ device; and
a key generator for performing a hashing algorithm on the password and the hint at
the ~~client~~ device to generate a key for decrypting the encrypted data.

Claim 16 (Currently Amended): A system, comprising:
means for obtaining a password through an interface to executable code transmitted to
a device;
means for sending encrypted data and a hint corresponding to the encrypted data from
a server to a ~~client~~ the device; and
means for performing a hashing algorithm on the password and the hint at the ~~client~~
device to generate a key for decrypting the encrypted data.

Claim 17 (Currently Amended): The system of claim 16, wherein the ~~system~~
~~includes~~ executable code is stored on a computer-readable storage medium.

Claim 18 (Currently Amended): The system of claim 16, wherein the system
~~includes~~ is configured to transmit the executable code embodied in a carrier wave.

Claim 19 (Currently Amended): A method, comprising:
receiving ~~identification of~~ information identifying encrypted data stored at a server;
sending a decryption downloadable ~~for~~ to a device, the decryption downloadable
deriving a key from a password and a hint ~~to a client~~;
sending ~~[[a]]~~ the hint corresponding to the encrypted data to the ~~client~~; ~~and~~ device;
and
deriving the key by hashing at least one of the hint and the password.

Claim 20 (Currently Amended): A system, comprising:
a decryption downloadable ~~for deriving~~ configured to derive a key by hashing at least
one of a password and a hint;
a memory configured to store encrypted data~~[[;]]~~ and a hint corresponding to the
encrypted data; and
a web server ~~for interfacing~~ configured to interface with ~~a client~~ the device, and ~~for~~
~~sending~~ send the decryption downloadable, the encrypted data, and the hint to the client.

Claim 21 (Currently Amended): A ~~client~~device based method, comprising:
obtaining a password through an interface to executable code transmitted to the device;
deriving a first secret from the password;
receiving a hint corresponding to data to be decrypted from a server;
deriving an intermediate index from the first secret and the hint; and
sending the intermediate index to the server, the intermediate index used to decrypt data stored on the server.

Claim 22 (Currently Amended): The method of claim 21, wherein deriving the first secret further includes hashing the password.

Claim 23 (Currently Amended): The method of claim 21, wherein deriving an intermediate index further includes hashing the first secret and the hint.

Claim 24 (Currently Amended): A system, comprising:
a user interface ~~for obtaining~~configured to obtain a password;
an index generator coupled to the user interface ~~for generating~~configured to generate
an intermediate index from a hint received from a server and a secret derived from the password; and
a communications engine coupled to the index generator ~~for sending~~configured to send the intermediate index to the server.

Claim 25 (Currently Amended): The system of claim 24, wherein the index generator is further configured to generate the intermediate index by hashing the hint and the secret.

Claim 26 (Currently Amended): A system, comprising;
means for obtaining a password through an interface to executable code transmitted to a device;
means for deriving a first secret from the password;
means for receiving a hint corresponding to data to be decrypted from a server;
means for deriving an intermediate index from the first secret and the hint; and
means for sending the intermediate index to the server, the intermediate index used to decrypt data stored at the server.

Claim 27 (Currently Amended): The system of claim 26, wherein the ~~system~~ includes the executable code is stored on a computer-readable storage medium.

Claim 28 (Currently Amended): The system of claim 26, wherein the system ~~includes~~ is configured to transmit the executable code embodied in a carrier wave.

Claim 29 (Currently Amended): A server-based method, comprising;
~~receiving an indication of encrypted data to be decrypted from a device, a request for~~
access to data stored at a server;
transmitting to ~~a client~~ the device a hint corresponding to the ~~indication data~~, and a decryption downloadable for deriving an intermediate index from a password and the hint;
receiving the intermediate index from the ~~client~~ device; and

deriving a decryption key from a second secret corresponding to the ~~user~~device and the intermediate index.

Claim 30 (Currently Amended): A system, comprising;
a memory configured to store a second secret corresponding to a ~~user~~device;
a decryption downloadable ~~for generating~~configured to generate an intermediate index from a password and a hint;
a web server ~~for receiving an indication of~~configured to receive information identifying encrypted data to be decrypted, ~~for transmitting~~transmit the decryption downloadable and a hint corresponding to the indication to ~~a client~~the device, and ~~for receiving~~receive an intermediate index from the ~~client~~device; and
a server-resident module ~~for deriving~~configured to derive a key for decrypting the encrypted data from the second secret and the intermediate index.